**BURSOR & FISHER, P.A.**
Sarah N. Westcot (State Bar No. 264916)
Stephen A. Beck (*pro hac vice*)
701 Brickell Avenue, Suite 1420
Miami, FL 33131
Telephone: (305) 330-5512
E-mail: swestcot@bursor.com
　　　　sbeck@bursor.com

*Counsel for Plaintiff*

# UNITED STATES DISTRICT COURT

## NORTHERN DISTRICT OF CALIFORNIA

| | |
|---|---|
| TAYLOR SMITH, individually and on behalf of all others similarly situated, | Case No. 3:24-cv-01703-RFL |
| Plaintiff, | **SECOND AMENDED CLASS ACTION COMPLAINT** |
| v. | |
| YETI COOLERS, LLC, | <u>JURY TRIAL DEMANDED</u> |
| Defendant. | |

SECOND AMENDED CLASS ACTION COMPLAINT – JURY TRIAL DEMANDED
CASE NO. 3:24-CV-01703-RFL

Plaintiff Taylor Smith ("Plaintiff"), individually and on behalf of all other persons similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself and her counsel, which are based on personal knowledge.

## NATURE OF THE ACTION

1.      This is a class action suit brought against Defendant Yeti Coolers, LLC ("Yeti" or "Defendant") for violating the California Invasion of Privacy Act ("CIPA").

2.       Defendant owns and operates the Yeti website, www.yeti.com (the "Website"), which sells Yeti-brand coolers, bags, and drinkware.

3.      Unbeknownst to Plaintiff and consumers, Defendant knowingly and willfully assists a third party with intercepting and recording confidential communications that contain consumers' sensitive financial information.

4.      Plaintiff brings this action for damages and other legal and equitable remedies resulting from Defendant's violation of the CIPA.

## PARTIES

5.      Plaintiff Taylor Smith is, and has been at all relevant times, a citizen of California who resides in Kelseyville, California.

6.      On June 14, 2023, Plaintiff purchased a Navy Rambler 36oz Water Bottle with Chug Cap from Defendant's Website.  When purchasing the product on the Website, Plaintiff entered her personally identifiable information, including her name, email address, home address, phone number, and zip code ("PII") and financial information, including credit card number, card issuer, expiration date, and CVC, to complete the transaction.

7.      Additionally, once Plaintiff entered the payment page on Defendant's Website to complete her transaction, Defendant assisted Adyen in installing software, known as a cookie, on Plaintiff's browser without her knowledge or consent.  This cookie allowed Adyen to surreptitiously monitor and intercept several additional pieces of PII, including the device, browser, and IP address associated with Plaintiff's transaction, as well as information related to whether she

1    manually entered her payment information, how much time she spent on the checkout page, and

2    how long it took for her to complete the transaction.

3           8.    This PII and financial information was then added to a unique profile internally

4    maintained by Adyen to track consumer purchasing behavior across its merchant network.

5           9.    When entering her PII and financial information on the Website, Plaintiff

6    reasonably expected that Defendant would keep this information private and not disclose it to third

7    parties.  However, Defendant disclosed such information to a third party, Adyen, without

8    Plaintiff's knowledge or consent.

9          10.    Adyen surreptitiously intercepted and recorded Plaintiff's PII and financial

10    information into its fraud prevention system to monetize and market these services to Defendant

11    and other merchants within Adyen's network.

12          11.    Plaintiff would not have completed a transaction on Defendant's Website if she

13    knew Yeti was disclosing her sensitive information to a third party.

14          12.    Defendant Yeti Coolers, LLC is a Delaware corporation with its principal place of

15    business at 7601 Southwest Parkway, Austin, Texas 78735.  Defendant develops, owns, and

16    operates yeti.com, a website that sells coolers, bags, and drinkware.

17                       **JURISDICTION AND VENUE**

18          13.    This Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A), as

19    amended by the Class Action Fairness Act of 2005 ("CAFA"),because this case is a class action

20    where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00,

21    exclusive of interest and costs, there are 100 members of the putative class, and Plaintiff, as well as

22    most members of the proposed class, are citizens of different states than Defendant.

23          14.    This Court has personal jurisdiction over Defendant.  First, by integrating the code

24    that allowed a third party to wiretap communications, Defendant acted intentionally.  Second,

25    Defendant knew that the harm would be felt in California because Defendant received billing and

26    mailing addresses each time a customer completed a purchase.  Third, Defendant expressly aimed

27    its conduct at California because Defendant, in the regular course of business, sells products

28    through its interactive website and causes those products to be delivered to the forum.  More

specifically, through the Website, Defendant sells products to California residents and ships those products to their home addresses. Defendant also allows residents to pick up their purchases from stores based in California, distributing products through roughly 700 locations.

15.     Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims occurred in this District.

**FACTUAL BACKGROUND**

16.     Each year, Americans spend more than $1 trillion on the internet, a figure that only continues to grow.[1] Despite this explosion in ecommerce, online retailers routinely fail to protect consumers' personal information, a failure that has reached "epidemic" levels[2] and shows no signs of slowing down.[3] Indeed, more than half of all Americans have suffered from a data breach,[4] costing each one an average of $146.[5] From these hacks, only fraudsters benefit, with identity thieves buying and selling personal information "by the millions" through illicit, online marketplaces.[6] There is such a glut of supply, in fact, that prices are relatively low; banking information costs around $100, for example, while credit card information costs as low as $10.[7]

---

[1] John Koetsier, *E-Commerce Retail Passed $1 Trillion For the First Time Ever*, FORBES (Jan. 28, 2023), https://www.forbes.com/sites/johnkoetsier/2023/01/28/e-commerce-retail-just-passed-1-trillion-for-the-first-time-ever/?sh=3191f5a836df.

[2] Apple, Report: 2.6 billion personal records compromised by data breaches in past two years – underscoring need for end-to-end encryption (Dec. 7, 2023), https://www.apple.com/newsroom/2023/12/report-2-point-6-billion-records-compromised-by-data-breaches-in-past-two-years/.

[3] Yves Audebert, Why authentication is good medicine for today's data breach epidemic (June 6, 2023), https://www.securitymagazine.com/articles/99443-why-authentication-is-good-medicine-for-todays-data-breach-epidemic.

[4] Kenneth Olmstead, et. al., *1. Americans' experiences with data security*, Pew Research Center (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/1-americans-experiences-with-data-security/

[5] IBM Security, Cost of a data breach Report (2020), https://www.ibm.com/security/digital-assets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf.

[6] NordVPN, Analyzing 4 million payment card details found on the dark web, https://nordvpn.com/research-lab/payment-card-details-theft/.

[7] Ryan Smith, *Revealed – how much is personal information worth on the dark web?*, Ins. Bus. Mag. (May 1, 2023), https://www.insurancebusinessmag.com/us/news/breaking-news/revealed--how-much-is-personal-information-worth-on-the-dark-web-444453.aspx#:~:text=Online%20banking%20login%20information%20costs,be%20purchased%20for%20about%20%241%2C000.

17. Despite these concerns, online retailers, like Defendant, intentionally disclose information to other companies that is sensitive and confidential. When completing a transaction, for example, a consumer often conveys details about her credit card and mailing address. Undoubtedly, consumers expect this information to be private and used only for the purposes of completing the transaction.

18. However, some merchants, like Defendant, assist third parties in intercepting this sensitive information to protect themselves from fraudulent transactions.

19. Once that information is received, third parties dissect it for inferences, taking anything they can glean and retooling it into products that they can sell to other customers.

20. Online retailers, like Defendant, have failed to protect consumers' personal information. Not only have they failed to protect that information, but they have also shared it voluntarily and intentionally, without obtaining consumer consent to do so.

21. Consumers in California have a right to know if private companies intend on sharing their sensitive information with third parties. Such disclosures are typically contained in a privacy policy on a company's website.

22. In fact, California law requires companies to "conspicuously post" their privacy policies. *See* Cal. Bus. & Prof. Code §§ 22575–79. As California courts have held, a notice is conspicuous if a reasonably prudent person would have seen it.

23. Such policies are crucial so that consumers are aware of what companies, like Defendant, are doing with their sensitive information.

24. As stated by California Attorney General Xavier Becerra, "California consumers have the right to know, the right to delete, and the right to opt-out of the sale of the personal information collected by businesses."
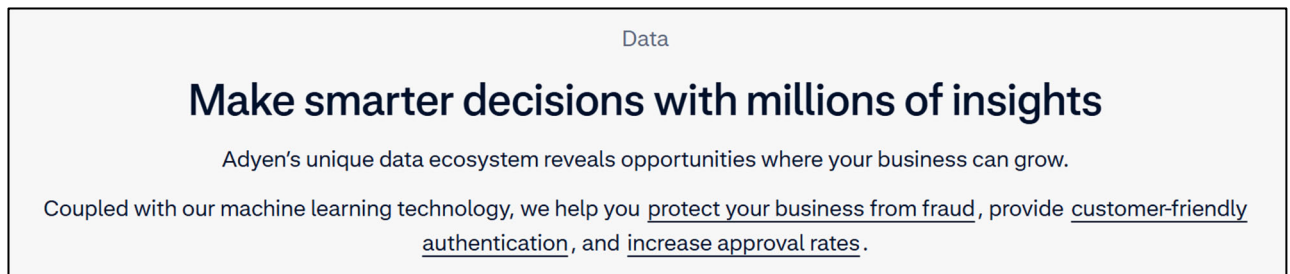
25. This does not stop some companies, like Defendant, from disclosing their customers' sensitive information with third parties without their knowledge or consent.

**Adyen's Payment Processing Services**

26.    Adyen, a Dutch payment company, offers merchants an online payment processing platform which merchants can integrate into their website for the purported purpose of processing consumer purchases.[8]

27.    However, Adyen does not merely process transactions.  Instead, Adyen monetizes the PII and financial information it intercepts from third party websites by indefinitely storing and incorporating it into its fraud prevention network.

28.    Adyen extensively markets these unique features and services to distinguish itself from its competitors:

**Figure 1**:

Data

## Make smarter decisions with millions of insights

Adyen's unique data ecosystem reveals opportunities where your business can grow.

Coupled with our machine learning technology, we help you protect your business from fraud, provide customer-friendly authentication, and increase approval rates.

29.    This vast network of data allows Adyen to provide additional services to merchants, including services related to risk management.[9]

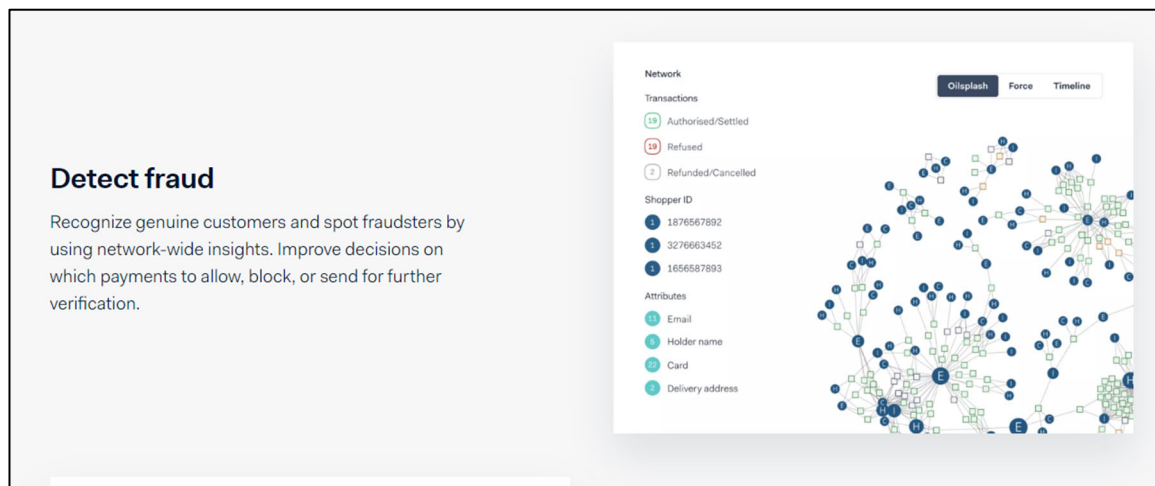30.    These risk management services are designed to protect merchants, rather than consumers, from fraud.

---

[8] https://www.adyen.com/online-payments.

[9] https://www.adyen.com/risk-management.

**Figure 2:**



31.     For example, Adyen allows merchants to access its "network-wide insights" to detect fraud:

**Figure 3:**



32.     Adyen fuels its consumer insights and data ecosystem through the interception of consumer data.  Adyen intercepts this data in two ways.

33.     Adyen primarily relies on intercepting PII and financial information when customers complete transactions on a merchant's website.  This is done when a customer enters their data in the payment fields on a merchant's website.  However, Adyen also instructs its merchants to install a software code, known as a cookie, on consumers' browsers in order to intercept additional data points, including the consumer's network, device, and IP address, as well as information related to whether the customer manually enters their payment information, how

much time they spend on the checkout page, and how long it takes for them to complete a transaction, as shown in Figure 4.
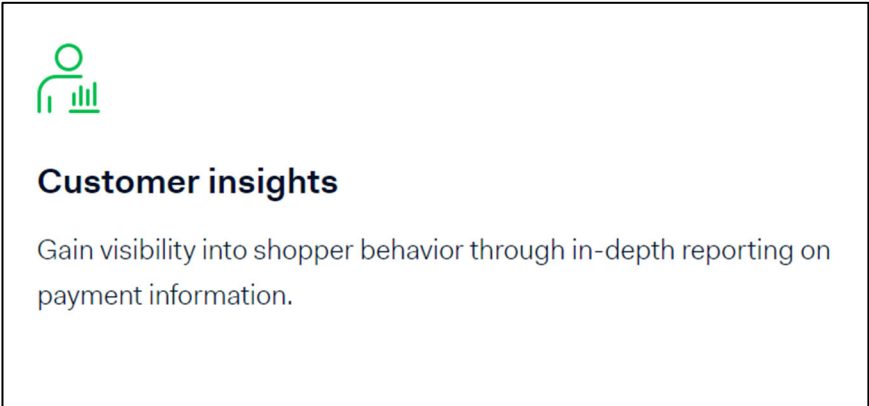
**Figure 4**:

| Data category | Example | Domain | Purpose | Lifetime |
|---|---|---|---|---|
| Cookie | `_RP_UID` | checkoutshopper-live.adyen.com | This cookie is used to track users, and helps identify suspicious browsing and/or purchasing activity. | 30 days in the browser |
| Device information | Attributes about the users' device. For example **Browser Type**, **Device Model**, **IP Address**, **Operating System**, **User Agent** and other information. | Checkout API ↗ | Collecting device information helps identify suspicious user behavior or transaction patterns. | Indefinite |
| Behavior information | How much time a shopper spent on the checkout page, if they copied and pasted payment details, and how long it took the shopper to complete certain actions like filling in a field. | Checkout API ↗ | Collecting behavior information lets Adyen analyze and identify suspicious user behavior and transaction patterns. | Indefinite |

34.    Ayden uses this data to fuel its risk management services, which allow merchants to gain valuable insights into consumers' purchasing history by tracking and recording consumers' purchases across devices and networks.

35.    For example, once this data is intercepted, Adyen then organizes it by creating unique consumer profiles for every customer that completes a transaction.  Such data is indefinitely stored into Adyen's data ecosystem, including its Shopper DNA and Customer Insights features. Adyen monetizes this vast network of data for the fraud prevention services it offers to merchants.

**Figures 5 and 6**:

**Customer insights**

Gain visibility into shopper behavior through in-depth reporting on payment information.

| Shopper DNA | Flag fraudulent transactions based on real-time data by identifying shoppers across devices, networks, and identities. |
|---|---|

36.    Adyen has built this vast network of consumer data by intercepting and indefinitely storing consumer information every time a consumer completes a transaction on a website that hosts its payment platform.

37.    This network allows Adyen to identify consumers across devices, networks, and identities and share this information with the merchants it partners with.

38.    The fraud prevention services offered by Adyen go far beyond routine commercial behavior.  In fact, the tools and services offered by Adyen are how it differentiates itself from its competitors.  Most payment processors lack the robust and unique data network offered by Adyen.

39.    Such services are incredibly valuable to merchants like Defendant.  Adyen aggressively markets these services to merchants, including Defendant.

40.    Adyen encourages companies to "[t]ake your business beyond the payment" by utilizing the advanced services they provide.[10]

41.    During the integration process, Adyen explains to companies, like Defendant, how their fraud prevention services operate, including where and how they receive the data that fuels their insights.

**Defendant's Use of Adyen's Services**

42.    Consumers visit Defendant's Website to make online purchases for coolers, bags, and drinkware.

43.    Defendant integrated Adyen's payment platform on its Website to process customer transactions and protect Defendant from fraudulent transactions.

44.    Defendant's Website does not include any identifying information or identification to alert consumers that their transactions are being processed by a third party.

---

[10] https://www.adyen.com/web-payments.

45.     Specifically, there is no branding on the payment screens indicating that Adyen is involved, and consumers cannot tell that Adyen is obtaining or storing sensitive information, including financial information.

46.     Moreover, Defendant does not alert consumers as to its data sharing practices or that their sensitive information is being shared with and indefinitely stored by a third party.

**Figures 7-9:**

47.    Consequently, consumers think they are only sending their sensitive PII and financial information to Defendant.

48.    Additionally, once Defendant's customers enter the payment page shown in Figures 7-9, Defendant assists Adyen in installing a cookie on its customers browser.  Adyen then surreptitiously intercepts additional identifying information, including their device, network, and IP address associated with their transaction, as well as information related to whether they manually entered their payment information, how much time they spent on the checkout page, and how long it took for them to complete the transaction.

49.    Adyen then organizes this information by creating unique consumer profiles, which Defendant can use to identify customers across devices and networks.

50.    Adyen then monetizes this consumer information by incorporating it into its database and marketing its fraud prevention services (which utilize this data) to other merchants.

51.    However, consumers are left unaware that such practices are even occurring.

52.    Defendant is aware of the purposes for which Adyen collects consumers' sensitive and private information because Defendant is knowledgeable of and benefiting from Adyen's fraud prevention services.

53.    Defendant is aware that it fails to obtain consent from its customers to share their sensitive PII and financial information with third parties.  Defendant knows that it is unlawful for

Adyen to obtain and utilize consumers' sensitive PII and financial information for its own benefit without consumers' consent to do so.

54.    Defendant chose to integrate Adyen's payment processing and fraud prevention software onto its Website because of the advanced features it offers.  Defendant knows that the PII and financial information it allows Adyen to intercept from its Website will be indefinitely stored and incorporated into Adyen's fraud prevention services because Adyen has explained to Defendant that this is how its services function.  Nonetheless, Defendant assisted Adyen in intercepting and storing its customers' sensitive PII and financial information to protect itself from fraudulent transactions.

55.    At no time are consumers informed nor do consumers consent to their sensitive information being disclosed and used in this manner.

## CLASS ALLEGATIONS

56.    **Class Definition**: Plaintiff seeks to represent a class of similarly situated individuals defined as all persons in California who made a purchase from Defendant's website, www.yeti.com (the "Class").

57.    Subject to additional information obtained through further investigation and discovery, the above-described Class may be modified or narrowed as appropriate, including through the use of multi-state subclasses.

58.    **Numerosity (Fed. R. Civ. P. 23(a)(1))**:  At this time, Plaintiff does not know the exact number of members of the Class.  However, given the popularity of Defendant's website, the number of persons within the Class is believed to be so numerous that joinder of all members is impractical.

59.    **Commonality and Predominance (Fed. R. Civ. P. 23(a)(2), 23(b)(3))**:  There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class that predominate over questions that may affect individual members of the Class include:

(a)    whether Defendant collected Plaintiff's and the Class's PII;

(b)    whether Defendant collected Plaintiff's and the Class's financial

information;

(c)    whether Defendant unlawfully disclosed and continues to disclose its users'

PII and financial information in violation of the CIPA;

(d)    whether Defendant's disclosures were committed knowingly;

(e)    whether Defendant disclosed Plaintiff's and the Class's PII and financial

information without consent;

(f)    whether Defendant intentionally recorded Plaintiff and Class members'

communications under the CIPA; and

(g)    whether Plaintiff and Class members' PII and financial information are

content under the CIPA.

60.    **Typicality (Fed. R. Civ. P. 23(a)(3))**:  Plaintiff's claims are typical of those of the

Class because Plaintiff, like all members of the Class, placed an order on Defendant's Website and

had her PII and financial information collected and disclosed by Defendant, and had her

communications recorded by Defendant, without her consent.

61.    **Adequacy (Fed. R. Civ. P. 23(a)(4))**: Plaintiff has retained and is represented by

qualified and competent counsel who are highly experienced in complex consumer class action

litigation, including litigation concerning the CIPA.  Plaintiff and her counsel are committed to

vigorously prosecuting this class action.  Moreover, Plaintiff is able to fairly and adequately

represent and protect the interests of the Class.  Neither Plaintiff nor her counsel have any interest

adverse to, or in conflict with, the interests of the absent members of the Class.  Plaintiff has raised

viable statutory claims of the type reasonably expected to be raised by members of the Class, and

will vigorously pursue those claims.  If necessary, Plaintiff may seek leave of this Court to amend

this Class Action Complaint to include additional representatives to represent the Class, additional

claims as may be appropriate, or to amend the definition of the Class to address any steps that

Defendant took.

62.    **Superiority (Fed. R. Civ. P. 23(b)(3))**:  A class action is superior to other available

methods for the fair and efficient adjudication of this controversy because individual litigation of

1   the claims of all members of the Class is impracticable.  Even if every member of the Class could

2   afford to pursue individual litigation, the court system could not.  It would be unduly burdensome

3   to the courts in which individual litigation of numerous cases would proceed.  Individualized

4   litigation would also present the potential for varying, inconsistent or contradictory judgments, and

5   would magnify the delay and expense to all parties and to the court system resulting from multiple

6   trials of the same factual issues.  By contrast, the maintenance of this action as a class action, with

7   respect to some or all of the issues presented herein, presents few management difficulties,

8   conserves the resources of the parties and of the court system and protects the rights of each

9   member of the Class.  Plaintiff anticipates no difficulty in the management of this action as a class

10  action.

## CAUSES OF ACTION

### COUNT I
**Violation of the California Invasion of Privacy Act,
Cal. Penal Code § 631**

63.     Plaintiff repeats the allegations contained in the paragraphs above as if fully set

forth herein and brings this count individually and on behalf of the members of the Class.

64.     The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§

630 to 638.  CIPA begins with its statement of purpose – namely, that the purpose of CIPA is to

"protect the right of privacy of the people of [California]" from the threat posed by "advances in

science and technology [that] have led to the development of new devices and techniques for the

purpose of eavesdropping upon private communications . . . ."  Cal. Penal Code § 630.

65.     A person violates California Penal Code § 631(a), if:

> by means of any machine, instrument, or contrivance, or in any other
> manner, [s/he] intentionally taps, or makes any unauthorized connection,
> whether physically, electrically, acoustically, inductively, or otherwise,
> with any telegraph or telephone wire, line, cable, or instrument, including
> the wire, line, cable, or instrument of any internal telephonic
> communication system, or [s/he] willfully and without the consent of all
> parties to the communication, or in any unauthorized manner, reads, or
> attempts to read, or to learn the contents or meaning of any message,
> report, or communication while the same is in transit or passing over any
> wire, line, or cable, or is being sent from, or received at any place within
> this state; or [s/he] uses, or attempts to use, in any manner, or for any

1

2

purpose, or to communicate in any way, any information so obtained . . . .

Cal. Penal Code § 631(a).

3

4

66.     Further, a person violates § 631(a) if s/he "aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned" in the preceding paragraph. *Id.*

5

6

7

67.     To avoid liability under § 631(a), a defendant must show it had the consent of <u>all</u> parties to a communication.

8

9

10

11

68.     At all relevant times, Defendant aided, agreed with, and conspired with Adyen to track and intercept Plaintiff's and Class Members' internet communications while accessing www.yeti.com.  These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

12

13

14

69.     Defendant, when aiding and assisting Adyen's wiretapping and eavesdropping, intended to help Adyen learn some meaning of the content in the form fields entered by Plaintiff and Class members.

15

16

17

70.     The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Adyen's payment platform falls under the broad catch-all category of "any other manner":

18

19

(a)     The computer codes and programs Adyen used to track Plaintiff and Class Members' communications while they were navigating www.yeti.com;

20

(b)     Plaintiff's and Class Members' browsers;

21

(c)     Plaintiff's and Class Members' computing and mobile devices;

22

23

24

(d)     The computer codes and programs used by Adyen to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit www.yeti.com; and

25

26

27

(e)     The plan Adyen carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile application to visit www.yeti.com.

28

71.    The information that Defendant transmitted using Adyen's payment platform constituted sensitive and confidential personally identifiable information.

72.    As demonstrated hereinabove, Defendant violated CIPA by aiding and permitting third parties to receive its customers' sensitive and confidential online communications through www.yeti.com without their consent.

As a result of the above violations, Defendant is liable to Plaintiff and other Class Members in the amount of, the greater of, $5,000 dollars per violation or three times the amount of actual damages. Additionally, Cal. Penal Code § 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages." Under the statute, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Defendant in the future.

**COUNT II**
**Violation of the California Invasion of Privacy Act**
**Cal. Penal Code § 632**

73.    Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein.

74.    CIPA § 632(a) prohibits an entity from:

intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio.

75.    The following items constitute "an electronic amplifying or recording device" under CIPA:

(a)    The computer codes and programs Adyen used to track Plaintiff and Class Members' communications while they were navigating www.yeti.com;

(b)    Plaintiff's and Class Members' browsers;

(c)    Plaintiff's and Class Members' computing and mobile devices;

(d)     The computer codes and programs used by Adyen to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a browser to visit www.yeti.com; and

(e)     The plan Adyen carried out to effectuate its tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser or mobile application to visit www.yeti.com.

76.     The data collected on Defendant's website constitutes "confidential communications," as that term is used in Section 632, because Class Members had objectively reasonable expectations of privacy with respect to their PII and financial information.

77.     Defendant is liable for aiding and abetting violations of Section 632 by the third-party vendors.

78.     Pursuant to Cal. Penal Code § 637.2, Plaintiff and Class members have been injured by the violations of Cal. Penal Code § 632(a), and each seek damages of $5,000 for each of Defendant's violations.

<div align="center">

**COUNT III**
**Invasion Privacy Under California's Constitution**

</div>

79.     Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class.

80.     Plaintiff and Class Members have an interest in: (1) precluding the dissemination and/or misuse of their sensitive, confidential online communications; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff's and Class Members' knowledge or consent.

81.     At all relevant times, by using Adyen's payment platform to record and communicate consumers' sensitive and confidential online communications, Defendant intentionally invaded Plaintiff's and Class Members' privacy rights under the California Constitution.

82.    Plaintiff and Class Members had a reasonable expectation that their sensitive and confidential online communications, identities, and financial information would remain confidential and that Defendant would not install wiretaps on www.yeti.com.

83.    Plaintiff and Class Members did not authorize Defendant to record and transmit Plaintiff's and Class Members' sensitive and confidential online communications.

84.    This invasion of privacy was serious in nature, scope, and impact because it related to their sensitive and confidential online communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

85.    Accordingly, Plaintiff and Class Members seek all relief available for invasion of privacy claims under California's Constitution.

## PRAYER FOR RELIEF

WHEREFORE, Plaintiff seeks a judgment against Defendant, individually and on behalf of all others similarly situated, as follows:

(a)    For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;

(b)    For an order declaring that Defendant's conduct violates the statutes referenced herein;

(c)    For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(d)    An award of statutory damages to the extent available;

(e)    For punitive damages, as warranted, in an amount to be determined at trial;

(f)    For prejudgment interest on all amounts awarded;

(g)    For injunctive relief as pleaded or as the Court may deem proper; and

(h)    For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

## JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

Dated:  November 8, 2024

**BURSOR & FISHER, P.A**.

By:  ___*/s/ Sarah N. Westcot*___

Sarah N. Westcot (State Bar No. 264916)
Stephen A. Beck (*pro hac vice*)
701 Brickell Avenue, Suite 1420
Miami, FL 33131
Telephone: (305) 330-5512
E-mail: swestcot@bursor.com
   sbeck@bursor.com

*Counsel for Plaintiff*